

**REMARKS / ARGUMENTS**

The present application includes pending claims 1-41, all of which have been rejected. The Applicant respectfully submits that the claims define patentable subject matter.

Claims 1-41 stand rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent Publication No. 2002/0001386, issued to Akiyama (hereinafter, Akiyama). The Applicant respectfully traverses these rejections at least for the reasons previously set forth during prosecution and at least based on the following remarks.

**I. Examiner's "Response to Arguments" in the Final Office Action**

The Examiner states the following in the Final Office Action:

Examiner respectfully disagrees with applicant's remark and still maintains that Akiyama discloses generating at a first location (Fig.29, This is a broadcast station where the contents, keys and digital signature for contact information etc, are generated and then sent to receivers) a digital signature (Fig. 5, "Digital signature") of a secure key to obtain a digitally signed secure key (Fig. 5, "work keys", also at paragraph 0107, "The digital signature is information used to check the authenticity of the contract information, and is used to prevent tampering.", also at paragraph 0107, "The contract information is made up of, e.g., a receiver 10, channel contract information, the number n of work keys, n pairs of work keys and work key identifiers, and digital signature"). So, *since the contract information contains work keys, which can be interpreted as "secure key", and digital signature is generated for entire contract information, which include work keys. When the digital signature is generated for entire contract information we can interpret that as*

Application No. 10/769,173  
Reply to Office Action of June 21, 2007

*signed contract information and since work keys are also part of contract information they can also be interpreted as signed work keys as required by claim 1.* Also at paragraphs 0112, 0113, 0114 and 0115 goes into more details of how the digital signature can be generated. Therefore, Akiyama clearly teaches this claimed limitation.

See the Final Office Action at pages 2-3 (emphasis added). The Applicant respectfully disagrees with the above italicized argument, and submits that the Examiner's interpretations are without any support in the reference and are contrary to what is disclosed by the reference.

Referring to Figures 1 and 5 of Akiyama, Akiyama specifically discloses that the digital signature from the contract information of Figure 5 is separately authenticated by the contract information certifying device 107, and it is not used for signing any of the work keys within the contract information. More specifically, the contract information certifying device 107 certifies or authenticates the digital signature using key information stored in the digital signature authentication key storage 108. If authentication fails, the device 107 sends back an error message via the individual information transceiver 102. If authentication succeeds, the device 107 stores channel contract information contained in the decrypted contract information in the contract information storage 121, and then sends a receipt acknowledgement indicating that update of contract information has terminated normally via the individual information transceiver 102. See Akiyama at paragraph 0111. Akiyama does not disclose or suggest that the

Application No. 10/769,173  
Reply to Office Action of June 21, 2007

digital signature in the contract information of Figure 5 is used in any way to sign the work keys. Therefore, the Examiner's interpretations above are erroneous.

The Applicant maintains that Akiyama does not disclose or suggest at least the limitation of "generating at a first location a digital signature of a secure key to obtain a digitally signed secure key," as recited by the Applicant in independent claim 1.

Furthermore, the Final Office Action states the following:

Note: individual control packets contains encrypted contract information (Paragraph 0106, "The individual control packet is comprised of an information identifier, master key identifier, and encrypted contract information, as shown in FIG. 7."), and as established above, contract information contains work keys, as a result, when control packet is transmitted, it contains the signed work keys as well, and thus we can interpret that signed work keys are transmitted from a broadcast device depicted in Fig. 29. Therefore, Akiyama clearly teaches this claimed limitation as well.

See the Final Office Action at pages 3-4. The Applicant points out that paragraph 0167 of Akiyama discloses transmission processing information for individual control packets. Furthermore, paragraph 0106 of Akiyama discloses that the individual control packets contain encrypted contract information. The Applicant points out that Akiyama discloses that **the work keys within the contract information are only encrypted and none of the contract information, including the work keys, is in fact signed to generate a digitally signed secure key.** As already explained above, the digital signature within the contract

Application No. 10/769,173  
Reply to Office Action of June 21, 2007

information is separately authenticated and it is not used to sign any of the remaining information within the contract information of Akiyama.

Therefore, the Applicant maintains that Akiyama does not disclose or suggest at least the limitation of "transmitting the digitally signed secure key from the first location," as recited by the Applicant in independent claim 1.

## **REJECTION UNDER 35 U.S.C. § 102**

### **II. Akiyama Does Not Anticipate Claims 1-41**

The Applicant now turns to the rejection of claims 1-41 under 35 U.S.C. 102(b) as being anticipated by Akiyama. With regard to the anticipation rejections under 102(b), MPEP 2131 states that "[a] claim is anticipated only if **each and every element** as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." See Manual of Patent Examining Procedure (MPEP) at 2131 (internal citation omitted). Furthermore, "[t]he identical invention must be shown in as complete detail as is contained in the ... claim." See id. (internal citation omitted).

#### **A. Rejection of Independent Claim 1 under 35 U.S.C. § 102(b)**

With regard to the rejection of independent claim 1 under 102(b), the Applicant submits that Akiyama does not disclose or suggest at least the limitation

Application No. 10/769,173  
Reply to Office Action of June 21, 2007

of "generating at a first location a digital signature of a secure key to obtain a digitally signed secure key," as recited by the Applicant in independent claim 1.

Regarding claim 1, the Final Office Action states the following:

Akiyama discloses a method for secure key authentication, the method comprising:

generating at a first location (Fig.29, This is a broadcast station where the contents, keys and digital signature for contact information etc, are generated and then sent to receivers) a digital signature (Fig. 5, "Digital signature") of a secure key to obtain a digitally signed secure key (Fig. 5, "work keys", also at paragraph 0107, 'The digital signature is information used to check the authenticity of the contract information, and is used to prevent tampering.', also at paragraph 0107, "The contract information is made up of, e.g., a receiver ID, channel contract information, the number n of work keys, n pairs of work keys and work key identifiers, and digital signature").

and transmitting the digitally signed secure key from the first location (Paragraph 0167, "The transmission processing operation of an individual control packet by the information distributor apparatus shown in FIG. 29... "). Note: individual control packets contains encrypted contract information (Paragraph 0106, "The individual control packet is comprised of an information identifier, master key identifier, and encrypted contract information, as shown in FIG. 7."), and as established above, contract information contains work keys, as a result, when control packet is transmitted, it contains the signed work keys as well, and thus we can interpret that signed work keys are transmitted from a broadcast device depicted in Fig. 29.

See the Final Office Action at page 5. The Examiner is referred to paragraph 0112 of Akiyama, which states the following, in relevant portions:

[t]he contract information shown in FIG. 5 except for the digital signature is sequentially encrypted for respective blocks using the secret key, and the last block is used as a digital signature.

See Akiyama at paragraph 0112. Therefore, in Akiyama **the contract information, which includes a plurality of work keys, is only encrypted using the secret key. Akiyama does not disclose or suggest that the work keys are also being signed** so as to generate digitally signed secure keys, as recited in Applicant's claim 1. **The digital signature from the contract information of Figure 5 is separately authenticated, and is not used for signing any of the work keys within the contract information.**

For example, referring to Figures 1 and 5 of the Akiyama reference, the Applicant points out that the contract information certifying device 107 is used to authenticate the digital signature in the contract information of Figure 5. For example, **the contract information certifying device 107 certifies or authenticates the digital signature using key information stored in the digital signature authentication key storage 108.** If authentication fails, the device 107 sends back an error message via the individual information transceiver 102. If authentication succeeds, the device 107 stores channel contract information contained in the decrypted contract information in the contract information storage 121, and then sends a receipt acknowledgement indicating that update of contract

information has terminated normally via the individual information transceiver 102.

See Akiyama at paragraph 0111.

Therefore, the Applicant maintains that Akiyama does not disclose or suggest at least the limitation of "generating at a first location a digital signature of a secure key to obtain a digitally signed secure key," as recited by the Applicant in independent claim 1.

Furthermore with regard to the rejection of independent claim 1 under 102(b), the Applicant submits that Akiyama does not disclose or suggest at least the limitation of "transmitting the digitally signed secure key from the first location," as recited by the Applicant in independent claim 1. Referring to Figure 1 of Akiyama, **the individual control information transceiver 102 only transmits error messages out of the apparatus 100.** See Akiyama at paragraphs 0110 and 0111. As it is clearly seen from Figure 1 of the reference, **information coming out of the contract information certifying device 107 is only communicated to storage devices 106, 108 or 121, and it is not transmitted by the transceiver 102.** In addition, paragraph 0106 of Akiyama discloses that the individual control packets contain encrypted contract information. The Applicant points out that **Akiyama discloses that the work keys within the contract information are only encrypted and none of the contract information, including the work keys, is in fact signed to generate a digitally signed secure key.** As already explained above, the digital signature within

Application No. 10/769,173  
Reply to Office Action of June 21, 2007

**the contract information is separately authenticated and it is not used to sign any of the remaining information within the contract information of Akiyama.**

Therefore, the Applicant maintains that Akiyama does not disclose or suggest at least the limitation of "transmitting the digitally signed secure key from the first location," as recited by the Applicant in independent claim 1.

Accordingly, independent claim 1 is not anticipated by Akiyama and is allowable. Independent claims 11, 21 and 32 are similar in many respects to the method disclosed in independent claim 1. Therefore, the Applicant submits that independent claims 11, 21 and 32 are also allowable over the references cited in the Office Action at least for the reasons stated above with regard to claim 1.

**B. Rejection of Dependent Claims 2-10, 12-20, 22-31 and 33-41**

Based on at least the foregoing, the Applicant believes the rejection of independent claims 1, 11, 21 and 32 under 35 U.S.C. § 102(b) as being anticipated by Akiyama has been overcome and requests that the rejection be withdrawn. Additionally, claims 2-10, 12-20, 22-31 and 33-41 depend from independent claims 1, 11, 21 and 32, respectively, and are, consequently, also respectfully submitted to be allowable.

Application No. 10/769,173  
Reply to Office Action of June 21, 2007

The Applicant also reserves the right to argue additional reasons beyond those set forth above to support the allowability of claims 2-10, 12-20, 22-31 and 33-41.

Application No. 10/769,173  
Reply to Office Action of June 21, 2007

**CONCLUSION**

Based on at least the foregoing, the Applicant believes that all claims 1-41 are in condition for allowance. If the Examiner disagrees, the Applicant respectfully requests a telephone interview, and requests that the Examiner telephone the undersigned Attorney at (312) 775-8176.

The Commissioner is hereby authorized to charge any additional fees or credit any overpayment to the deposit account of McAndrews, Held & Malloy, Ltd., Account No. 13-0017.

A Notice of Allowability is courteously solicited.

Date: 21-AUG-2007

Respectfully submitted,



Ognyan Beremski, Esq.  
Registration No. 51,458  
Attorney for Applicant

McANDREWS, HELD & MALLOY, LTD.  
500 WEST MADISON STREET, 34TH FLOOR  
CHICAGO, ILLINOIS 60661  
(312) 775-8000

/ OIB